Cisco Systems, Inc. PIX 515 and PIX 515E

FIPS 140-2 Non-Proprietary Security Policy

Level 2 Validation

Document Version: Version 1.12

March 20, 2006

Introduction

Purpose

This is a non-proprietary Cryptographic Module Security Policy for the PIX 515 and PIX 515E from Cisco Systems, Inc., referred to in this document as the modules, appliances, or as previously stated. This security policy describes how modules meet the security requirements of FIPS 140-2 and how to run the modules in a FIPS 140-2 mode of operation.

This policy was prepared as part of the Level 2 FIPS 140-2 validation of the PIX 515 and PIX 515E.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/cryptval/.

References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Cisco Systems, Inc. website (http://www.cisco.com) contains information on the full line of products from Cisco Systems, Inc.
- The NIST Cryptographic Module Validation Program website (http://csrc.ncsl.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

Document Organization

The Security Policy document is one document in a complete FIPS 140-2 Submission Package. In addition to this document, the complete Submission Package contains:

- Vendor Evidence
- Finite State Machine
- Other supporting documentation as additional references

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Cisco Systems, Inc. and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact

PIX 515 AND PIX 515E FROM CISCO SYSTEMS, INC.

Overview

The market-leading Cisco PIX Security Appliance Series deliver robust user and application policy enforcement, multi-vector attack protection, and secure connectivity services in cost-effective, easy-to-deploy solutions. Cisco PIX Security Appliances provide comprehensive security, performance, and reliability for network environments of all sizes.

These purpose-built appliances provide multiple integrated security and networking services, including:

- Advanced application-aware firewall services
- Market-leading voice over IP (VoIP) and multimedia security
- Robust site-to-site and remote-access IPSec VPN connectivity
- Award-winning resiliency
- Intelligent networking services
- Flexible management solutions

The PIX 515 and 515E Security Appliances are validated with the VPN Acceleration Card+ (VAC+), which delivers high-performance, hardware-accelerated IP Security (IPSec) VPN support for state-of-the-art international cryptographic standards and highly scalable VPN tunnel aggregation in a solution that comes integrated with, or as an upgrade for, most models of the market-leading Cisco PIX Security Appliance Series. Ranging from solutions for small to midsize businesses (SMBs) to large enterprises and service providers, the Cisco PIX Security Appliance Series offers extensible platforms that provide robust, enterprise-class integrated network security services and solid investment protection. The Cisco PIX VAC+ takes full advantage of this extensibility and maximizes platform investment protection by offloading computationally intensive VPN cryptographic functions. This enables Cisco PIX Security Appliances to deliver higher-performance stateful inspection firewall services, advanced application and protocol inspection, inline intrusion protection, and robust multimedia and voice security services.

Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

No.	Area Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key management	2
8	Electromagnetic Interface/Electromagnetic Compatibility	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

Table 1 – Validation Level by Section

Physical Characteristics and Module Interfaces

Each appliance is a multi-chip standalone module, and the cryptographic boundary is defined as encompassing the "top," "front," "left," "right," and "bottom" surfaces of the case; all portions of the "backplane" of the case which are not designed to accommodate a removable interface or service card; and the inverse of the three-dimensional space within the case that would be occupied by an installed Service Card. The cryptographic boundary includes the connection apparatus between the Service Card and the motherboard/daughterboard that hosts the Service Card, but the boundary does not include the Service Card itself (except when a VAC+ is inserted into an available PIX Circuit Board Interface). In other words, the cryptographic boundary encompasses all hardware components within the case of the device except any installed modular Service Card (except when a VAC+ is inserted into an available PIX Circuit Board Interface).

Each module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their mapping are described in the following tables:

Physical Interface	FIPS 140-2 Logical Interface
10/100BaseTX Ethernet 0 10/100BaseTX Ethernet 1 WIC/VIC/HWIC Interfaces 0-1 Circuit Board Interfaces 0-1 Console Port	**Data Input Interface**
10/100BaseTX Ethernet 0 10/100BaseTX Ethernet 1 WIC/VIC/HWIC Interfaces 0-1 Circuit Board Interfaces 0-1 Console Port	**Data Output Interface**
10/100BaseTX Ethernet 0 10/100BaseTX Ethernet 1 WIC/VIC/HWIC Interfaces 0-1 Circuit Board Interfaces 0-1 Power Switch Console Port	**Control Input Interface**
10/100BaseTX Ethernet 0 10/100BaseTX Ethernet 0 100Mbps LED 10/100BaseTX Ethernet 0 ACT LED 10/100BaseTX Ethernet 1 10/100BaseTX Ethernet 1 100Mbps LED 10/100BaseTX Ethernet 1 ACT LED WIC/VIC/HWIC Interfaces 0-1 Circuit Board Interfaces 0-1 Power LED System Activity LED Network LED Console Port	**Status Output Interface**
Main Power Plug	**Power Interface**
USB Port **Serial Failover Interface**	**Unused**

Table 2 – 515/515E Physical Interface / Logical Interface Mapping

Roles and Services

The module can be accessed in one of the following ways.

- Console Port
- Telnet over IPsec
- SSH
- ASDM via HTTPS/TLS

As required by FIPS 140-2, there are two main roles in the module that operators may assume: a Crypto Officer role and User role. The module supports role-based authentication, and the respective services for each role are described below.

Crypto Officer Services

The Crypto Officer role is responsible for the configuration and maintenance of the module and authenticates from the **`enable`** command (for local authentication) or the **`login`** command (for AAA authentication) from the User services. The Crypto Officer services consist of the following:

- **Configure the Module**: define network interfaces and settings; set the protocols the module will support; enable interfaces and network services; set system date and time; load authentication information; and configure authentication servers, filters and access lists for interfaces and users, and privileges
- **Define Rules and Filters**: create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based on characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.
- **View Status**: view the configuration, routing tables, active sessions, use *gets* to view SNMP MIB statistics, health, temperature, memory status, packet statistics, review accounting logs, and view physical interface status.
- **Manage the Module**: log off users, shutdown or reload the module, view complete configurations, view full status, manage user rights, and restore configurations.
- **Set Encryption/Bypass**: set up the configuration tables for IP tunneling. Set keys and algorithms to be used for each IP range or allow plaintext packets to be sent from specified IP address.
- **Install Service Card**: remove tamper evident seals to install or replace Service Cards.

User Services

A User enters the system by accessing the console port with a terminal program or via IPSec protected telnet or SSH session to a LAN port. The module will prompt the User for their password. If the password is correct, the User is allowed entry to the executive program. The services available to the User role consist of the following:

- **Status Functions**: image version currently running, installed hardware components, and version of hardware installed
- **Network Functions**: initiate diagnostic network services (i.e., ping)

- **Directory Services**: display directory of files kept in flash memory

The services accessing the Critical Service Parameters (CSP)s, the type of access and which role accesses the CSPs are listed in the Table 3.

CSP/Role/Service Access Policy	Critical Security Parameter	CSP 1	CSP 2	CSP 3	CSP 4	CSP 5	CSP 6	CSP 7	CSP 8	CSP 9	CSP 10	CSP 11	CSP 12	CSP 13	CSP 14	CSP 15	CSP 16
Role/Service																	
User role																	
Status Functions		r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r
Network Functions		r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r
Directory Services		r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r
Crypto-Officer Role																	
Configure the Module		r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d
Define Rules and Filters		r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d
Status Functions																	
Manage the Module		r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d
Set Encryption/Bypass		r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d
Install Service Card																	

Table 3 – Role and Service Access to Security Relevant Data Items

Authentication Mechanisms

The module supports either a password or digital certificates for authenticating IPSec users. To log on to the appliances for management purposes, an operator must connect to it through one of the management interfaces (Console Port, SSH, Telnet, or ASDM) and provide a password.

Authentication Type	Strength
Username Password mechanism	Passwords must be a minimum of 6 characters (see Secure Operation section of this document). The password can consist of alphanumeric values, a-zA-Z0-9, yielding 62 choices per character. The probability of a successful random attempt is 1/62^6, which is less than 1/1,000,000. This is also valid for RADIUS or TACACS+ shared secret keys.
Certificate based authentication	The module supports a public key based authentication with 1024 and 2048 (for RSA) bit keys. A 1024-bit RSA key has at least 80-bits of equivalent strength. The probability of a successful random attempt is 1/2^80, which is less than 1/1,000,000. A 2048-bit RSA key has at least 112-bits of equivalent strength. The probability of a successful random attempt is 1/2^112, which is less than 1/1,000,000.

Table 4 – Estimated Strength of Authentication Mechanisms

Cryptographic Key Management

The appliances use a variety of Critical Security Parameters during operation. Below is a complete list of keys and CSPs used by various services and protocols:

#	Key / CSP Name	Generation / Algorithm	Description	Storage	Zeroization
1	RSA public/private keys	ANSI X9.31 / RSA	Identity certificates for the module itself and also used in IPSec, TLS, and SSH negotiations. The module supports 1024 and 2048 bit key sizes.	Private Key - NVRAM (plaintext) and RAM (plaintext) Public Key - NVRAM (plaintext) and RAM (plaintext)	Both private and public key can be zeroized by the erase flash: command and then rebooting the module. This command zeroizes the entire contents of the FLASH.
2	DSA public/private keys	ANSI X9.31 / DSA	Identity certificates for the module itself and also used in IPSec negotiations.	Private Key - NVRAM (plaintext) and RAM (plaintext)	Both private and public key can be zeroized by the erase flash: command and then rebooting the module. This command

				Public Key - NVRAM (plaintext) and RAM (plaintext)	zeroizes the entire contents of the FLASH.
3	Diffie-Hellman Key Pairs	ANSI X9.31 / DH	Key agreement for IKE, TLS, and SSH sessions	RAM (plaintext)	Resetting or rebooting the module
4	Public keys	DSA / RSA	Public keys of peers	RAM (plaintext)	Resetting or rebooting the module
5	TLS Traffic Keys	Generated using the TLS protocol (X9.31PRNG + HMAC-SHA1 + HMAC-MD5 + either DH or RSA) Algorithm: Also Triple DES & AES	Used in HTTPS connections	RAM (plaintext)	Resetting or rebooting the module
6	SSH Session Keys	ANSI X9.31 / Triple DES-AES	SSH keys	RAM (plaintext)	Resetting or rebooting the module
7	IPSec auth-entication keys	ANSI X9.31 / Triple DES-AES / DH	Exchanged using the IKE protocol and the public/private key pairs. These are Triple DES or AES keys.	RAM (plaintext)	Resetting or rebooting the module
8	IPSec traffic keys	ANSI X9.31 / Triple DES-AES / DH	Exchanged using the IKE protocol and the public/private key pairs. These are Triple DES or AES keys.	RAM (plaintext)	Resetting or rebooting the module
9	IKE pre-shared keys	Shared Secret	Entered by the Crypto-Officer in plaintext form and used for authentication during IKE	NVRAM (plaintext) and RAM (plaintext)	Deleting keys from the configuration via `erase flash:` command and then rebooting the module. This command zeroizes the entire contents of the FLASH.
10	IKE Auth-entication key	Generated using IKE (X9.31+HMAC-SHA1+DH). Algorithms: Triple DES, AES, SHA-1	Used to encrypt and authenticate IKE negotiations	RAM (plaintext)	Resetting or rebooting the module
11	IKE Encryption Key	Generated using IKE (X9.31+HMAC-SHA1+DH). Algorithms: Triple DES, AES, SHA-1	Used to encrypt IKE negotiations	RAM (plaintext)	Resetting or rebooting the module
12	RADIUS and TACACS+ shared secret keys	Shared Secret	Used for authenticating the RADIUS or TACACS+ server to the module and vice versa. Entered by the Crypto-Officer in plaintext form and stored in plaintext form.	NVRAM (plaintext) and RAM (plaintext)	Deleting keys from the configuration via `erase flash:` command and then rebooting the module. This command zeroizes the entire contents of the FLASH.
13	Usernames/ Passwords	Secret	Critical security parameters used to authenticate the	NVRAM (plaintext)	The passwords can be zeroized via the erase

			user/crypto-officer logging in on to the machine.	and RAM (plaintext)	flash: command and then rebooting the module. This command zeroizes the entire contents of the FLASH.
14	Certificates of Certificate Authorities (CAs)	ANSI X9.31	Necessary to verify certificates issued by them. So the CA's certificate should be installed before installing the certificate issued by it.	NVRAM (plaintext) and RAM (plaintext)	The CA certificates can be zeroized via the erase flash: command and then rebooting the module. This command zeroizes the entire contents of the FLASH.
15	PRNG Seed Key	Entropy	Seed key for X9.31 PRNG	RAM (plaintext)	Zeroized with generation of new seed
16	Failover Key	Pre-shared secret	Used to encrypt and authenticate LAN-based failover.	NVRAM (plaintext) and RAM (plaintext)	Deleting keys from the configuration via `erase flash:` command. This command zeroizes the entire contents of the FLASH and then rebooting the module.

Table 5 - Cryptographic Keys Used by the Module

Self-Tests

The modules include an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to insure all components are functioning correctly. The modules implement the following power-on self-tests:

Implementation	Tests Performed
Security Appliance Software	• Software/firmware Test • Bypass Test • DSA KAT (signature/verification) • RSA KAT (signature/verification) • RSA KAT (encrypt/decrypt) • AES KAT • Triple DES KAT • SHA-1 KAT • HMAC SHA-1 KAT • PRNG KAT
VAC+ (Broadcom 5823)	• DSA KAT (signature/verification) • RSA KAT (signature/verification) • AES KAT • Triple DES KAT • SHA-1 KAT • HMAC SHA-1 KAT

Table 6 - Module Power On Self Tests

The modules perform all power-on self-tests automatically at boot when FIPS mode is enabled. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The power-on self-tests

are performed after the cryptographic systems are initialized but prior to the initialization of the LANs; this prevents the module from passing any data during a power-on self-test failure. In the unlikely event that a power-on self-test fails, an error message is displayed on the console followed by a module reboot.

In addition, the modules also perform the following conditional self-tests:

Implementation	Tests Performed
Security Appliance Software	• Pairwise consistency test for RSA • Pairwise consistency test for DSA • Continuous Random Number Generator Test for the FIPS-approved RNG and non-approved RNGs. • Conditional Bypass test
VAC+ (Broadcom 5823)	• Pairwise consistency test for DSA

Table 7 - Module Conditional Self Tests

Mitigation of Other Attacks

The modules do not claim to mitigate any attacks in a FIPS-approved mode of operation.

SECURE OPERATION

The PIX 515 and PIX 515E meet FIPS 140-2 Level 2 requirements. This section describes how to place and keep the modules in a FIPS-approved mode of operation. Operating the modules without maintaining the following settings will remove the modules from the FIPS-approved mode of operation.

Crypto Officer Guidance – System Initialization

The modules were validated with Adaptive Security Appliance Software version 7.0.4 (file name: pix704.bin). This is the only allowable image for FIPS-approved mode of operation.

The Crypto Officer must configure and enforce the following initialization procedures:

1. Ensure the security context mode is set to single mode:

   ```
   (config)# mode single
   ```

2. Ensure the firewall mode is set to routed:

   ```
   (config)# no firewall transparent
   ```

3. Disable the console output of system crash information via the following command:

   ```
   (config)#crashinfo console disable
   ```

4. Enable “FIPS Mode” to allow the module to internally enforce FIPS-compliant behavior (e.g., run power-on self tests and bypass test)

   ```
   (config)#fips enable
   ```

5. Install Triple DES/AES licenses to require the module to use Triple DES and AES (for data traffic and SSH).
6. Disable password recovery

   ```
   (config)#no service password-recovery
   ```

7. Set the configuration register to bypass ROMMON prompt at boot

   ```
   (config)# config-register 0x10011
   ```

8. Define the failover key to ensure encryption of the link to redundant modules prior to enabling failover

```
(config)#failover key hex <key>
```

Note: Failover is not required for FIPS mode of operation. If failover is to be enabled, then the above configuration should be followed. Also, only LAN-based failover is allowed for FIPS mode of operation; serial link failover is not allowed in FIPS mode of operation. Failover should not be configured over the lowest-numbered interface (e.g., Ethernet 0); ports Ethernet 1 or above should be used. If the lowest-numbered interface is already implemented as the failover interface, the Crypto Officer should take the following action:

- Before upgrading to v7.0.4, copy the configuration to a location off the device
- Use a text editor to modify the interface configuration
- Change the failover cables to the specified failover interface
- Upgrade to v7.0.4 and reload the modified configuration

9. Enable AAA authorization for the console

```
(config-terminal)#aaa authentication serial console LOCAL
(config-terminal)#username <name> password <password>
```

10. Enable AAA authorization for SSH and Telnet:

```
(config-terminal)#aaa authentication ssh console LOCAL
(config-terminal)#aaa authentication telnet console LOCAL
```

11. Enable AAA authorization for Enable mode

```
(config-terminal)#aaa authentication enable console LOCAL
```

12. Specify Privilege Level 15 for Crypto Officer and Privilege Level 1 for User and set up username/password for each role:

```
(config-terminal)#username <name> password <password> privilege 15
(config-terminal)#username <name> password <password> privilege 1
```

13. Ensure passwords are at least 6 characters long.
14. All default passwords (e.g., enable, telnet) should be replaced with new passwords.
15. Apply tamper evident labels as described in the “Tamper Evidence” section below.

Note: The Crypto Officer may install any Service Card modules that only provide a physical interface (e.g., PIX-1FE, PIX-1GE-66, PIX-4FE-66).The PIX modules are validated only with the VPN Acceleration Card PLUS (VAC+) for cryptographic acceleration; the legacy VAC is not supported in FIPS approved mode of operation.

16. Reboot the module.

Crypto Officer Guidance – System Configuration

To operate in FIPS mode, the Crypto Officer must:

1. Assign users a Privilege Level of 1.
2. Define RADIUS and TACACS+ shared secret keys that are at least 6 characters long and secure traffic between the module and the RADIUS/TACACS+ server via IPSec tunnel.

   Note: this only if use of RADIUS/TACACS+ is configured
3. Configure the TLS protocol when using HTTPS to protect administrative functions. Due to known issues relating to the use of TLS with certain versions of the Java plugin, it is recommended that the customer upgrade to JRE 1.5.0_05 or later. The following configuration settings are known to work when launching ASDM in a TLS-only environment with JRE 1.5.0_05:

   - Configure the device to allow only TLSv1 packets via
     `(config)# ssl server-version tlsv1-only`
   - Uncheck SSL Version 2.0 in both the web browser and JRE security settings
   - Check TLS V1.0 in both the web browser and JRE security settings
4. Configure the module to use SSHv2. Note that all operators must still authenticate after remote access is granted.
5. Configure the module such that any remote connections via telnet are secured through IPSec.
6. Configure the module such that only FIPS-approved algorithms are used for IPSec tunnels.
7. Configure the module such that error messages can only be viewed by an authenticated Crypto Officer.
8. Configure SNMP v3 over a secure IPSec tunnel may be employed for authenticated, secure SNMP *gets* and *sets*. Since SNMP v2C uses community strings for authentication, only *gets* are allowed under SNMP v2C.
9. Disable the FTP, and TFTP servers as well as HTTP for performing system management.
10. Ensure that installed digital certificates are signed using FIPS approved algorithms (SHA-1).
11. Ensure that 512-bit and 768-bit RSA keys are not used.

12. Ensure that the DSA algorithm uses at least a 512-bit modulus.

Approved Cryptographic Algorithms

The appliances support many different cryptographic algorithms; however, only FIPS approved algorithms may be used. The following cryptographic algorithms are to be used:

- AES encryption/decryption
- Triple DES encryption/decryption
- SHA-1 hashing
- SHA-1 HMAC for hashed message authentication
- RSA signing and verifying
- DSA signing and verifying
- X9.31 for RNG
- TLS for Layer 7 security

Note: Pursuant to the DES Transition Plan and the approval of the *Withdrawal of Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard (DES); FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation*, the DES algorithm should not be used in FIPS approved mode of operation. The DES algorithm must not be used when the Triple DES/AES licenses are installed.

Each cryptographic implementation in the PIX Security Appliance Software and VAC+ module has achieved the following certifications:

Algorithm	Adaptive Security Appliance Software	VPN Acceleration Card+
AES	320	209
Triple DES	384	298
SHA-1	393	285
SHA-1 HMAC	124	15
RNG	143	Not supported
RSA	105	107
DSA	150	152

Table 8 - Algorithm Certificates

Non-FIPS Approved Algorithms

The modules implement the following non-FIPS-approved cryptographic algorithms:

- DES
- SSL
- RC4
- MD5
- MD5 HMAC

- Diffie-Hellman (allowed for use in FIPS mode) (key establishment methodology provides 80-bits or 96-bits of encryption strength)
- RSA encryption/decryption (allowed in FIPS mode for key transport) (key establishment methodology provides 80-bits or 112-bits of encryption strength)

Tamper Evidence

All CSPs are stored and protected within each appliance's tamper evident enclosure. The administrator is responsible for properly placing all tamper evident labels. The security labels recommended for FIPS 140-2 compliance are provided in the FIPS Kit. These security labels are very fragile and cannot be removed without clear signs of damage to the labels.

The Crypto Officer should inspect the tamper evident labels periodically to verify they are intact and the serial numbers on the applied tamper evident labels match the records in the security log.

Application of the serialized tamper evident labels is as follows:

PIX 515 and 515E

1. Turn off and unplug the system before cleaning the chassis and applying labels.
2. Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.
3. Apply a label on the front of the box such that the label covers the front plate and the top of the module's case. Apply a label to cover the module's side and bottom portions of the case.

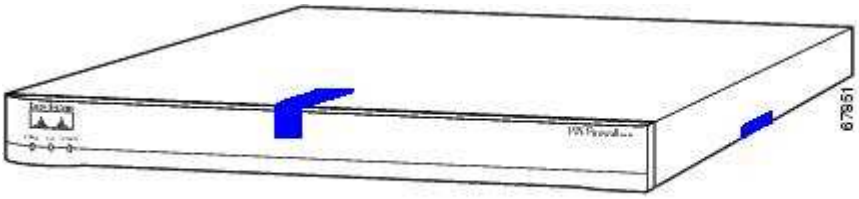

Figure 1 - PIX 515/515E Front Tamper Evident Label Placement

4. On the back of the module, apply labels to cover the interface slots. Also apply a label to cover the module's side and bottom portions of the case on the opposite side as in Step 3.

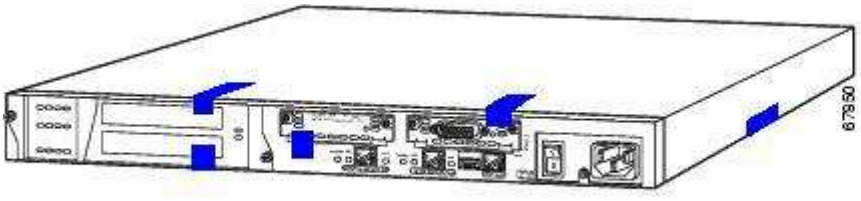

Figure 2 - PIX 515/515E Back Tamper Evident Label Placement

5. Record the serial numbers of the labels applied to the system in a security log.

The tamper evident seals are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the device will damage the tamper evident seals or the material of the module cover. Since the tamper evident seals have non-repeated serial numbers, they may be inspected for damage and compared against the applied serial numbers to verify that the module has not been tampered with. Tamper evident seals can also be inspected for signs of tampering, which include the following: curled corners, rips, and slices. The word "OPEN" may appear if the label was peeled back.

DEFINITION LIST

AES	Advanced Encryption Standard
ASA	Adaptive Security Appliance
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
DES	Data Encryption Standard
FIPS	Federal Information Processing Standard
HTTP	Hyper Text Transfer Protocol
KAT	Known Answer Test
LED	Light Emitting Diode
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
RAM	Random Access Memory
RSA	Rivest Shamir and Adleman method for asymmetric encryption
SCEP	Simple Certificate Enrollment Protocol
Service Card	A service card may provide additional interfaces, feature acceleration or additional services. Service cards may take a Circuit Board form factor for PIX appliances
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security